# Aula 08

# Firewall

Prof. Roitier Campos Gonçalves

# Conceito

Um firewall, ou filtro de pacotes, é um recurso utilizado para proteger uma máquina ou uma rede através do controle e filtragem dos pacotes/datagramas que entram ou que saem.

O firewall deve ser visto como uma ferramenta a mais para tornar sua rede segura, e não como a única ferramenta.

Tradicionalmente, um firewall atua nas camadas 3 e 4 do modelo ISO/OSI. Alguns são capazes de também atuar na camada de aplicação, mas são menos comuns devido à sua complexidade

# Firewalls podem:

- Proteger apenas um host.
  - Implementados na própria máquina;
  - Não exigem mudanças na topologia da rede.

- Proteger uma ou mais redes.
  - Atuam como roteador;
  - Exigem mudanças na topologia da rede: o tráfego da rede deve passar por ele.

# Tipos de firewalls

- Stateless:
  - Cada pacote é analisado sem levar em conta outros pacotes;
  - Não existe “conexão” (controle sobre o fluxo).

- Stateful
  - Guardam atributos de conexões;
  - Reconhecem “estados”;
  - No Linux: kernel > 2.4.x.

# Stateless

Firewalls que analisam cada pacote de maneira isolada, levando em conta apenas atributos dos cabeçalhos, como, por exemplo, endereços e portas de origem e destino. Esse tipo de firewall não tem como reconhecer se um determinado pacote está tentando estabelecer uma nova conexão ou se faz parte de uma conexão já estabelecida.

Além da necessidade de se criar duas regras, um atacante malicioso poderia acessar hosts atrás do firewall simplesmente utilizando conexões originadas na porta 80.

# Stateless: Regras

A criação de regras para firewalls desse tipo é mais complexa e menos precisa, porque o administrador precisa criar pares de regras para cada situação. Por exemplo, supondo que o administrador precise permitir que hosts de sua rede acessem páginas web na internet, seria necessário:

- Criar uma regra que permitisse pacotes com endereços de sua rede e portas de origem quaisquer (>1023), e destino qualquer e porta de destino 80.
- Criar uma regra com origem qualquer e porta de origem 80, com destino de sua rede e porta de destino qualquer (>1023).

# Stateful

Firewalls capazes de reconhecer e armazenar estados de conexões que passam por ele, como, por exemplo, fluxos TCP. Um firewall desse tipo pode decidir o que fazer com um pacote, baseado no estado desse pacote em relação a uma conexão.

Utilizando o exemplo anterior, o administrador teria de criar apenas a primeira regra e uma segunda regra genérica que permita a passagem dos pacotes que façam parte das conexões estabelecidas.

# Netfilter

Netfilter é o nome do código presente no kernel do Linux (>2.4.x), que implementa as funções de firewall. Para entender melhor como o netfilter funciona, será necessário estudar alguns conceitos utilizados por ele:

- Regras.
- Estados.
- Chains.
- Tabelas.

# Regras

Basicamente, uma regra é uma descrição do que fazer com que tipo de pacote. Cada regra possui um padrão de procura e uma ação, também chamada de alvo. Na criação de um padrão, utiliza-se praticamente qualquer campo dos cabeçalhos dos protocolos IP, ICMP, TCP e UDP. Além disso, dentro de uma conexão nesses padrões, é possível utilizar também os estados de um pacote.

Cada tipo de regra aceita um conjunto de ações possíveis. Pode-se aceitar, rejeitar, ignorar, modificar, registrar, marcar pacotes ou até mesmo fazer com que os pacotes sejam avaliados por outros conjuntos de regras. Veremos mais adiante algumas ações possíveis e como construir padrões para serem utilizados nas regras.

# ...Regras

Possui um padrão de casamento (match) e um alvo (target).

- Padrões de casamento (match):
  - Campos de cabeçalho.
  - Estados de conexões.

- Alvos (target):
  - Aceitar, rejeitar, ignorar, modificar, logar, chains.

# Estados

O netfilter é capaz de reconhecer o estado de uma conexão. Além de facilitar a configuração de regras, isso permite maior controle sobre o que passa pelo firewall.

Netfilter reconhece os seguintes estados:

- NEW: pacotes iniciais de um fluxo;
- ESTABLISHED: quando a resposta ao pacote inicial (NEW) chega ao firewall, os próximos pacotes desse fluxo passam a ser identificados como ESTABLISHED;
- RELATED: pacotes que de alguma maneira se relacionam a uma conexão já estabelecida. Ao se fazer uma conexão FTP, por exemplo, são abertas duas conexões: uma em que trafegam dados; e outra em que trafegam informações ou controle. Essa segunda conexão poderia ser vista pelo netfilter como sendo RELATED;
- INVALID: pacotes que, por alguma razão, não foram identificados

# Chains

Uma chain é uma estrutura que contém regras. O netfilter possui dois tipos de chains:

- **Chains do sistema:** denominadas PREROUTING, INPUT, FORWARD, OUTPUT e POSTROUTING, estão ligadas a pontos especiais no caminho que os pacotes percorrem ao entrar e sair da máquina.

- **Chain de usuário:** só será percorrida se alguma chain do kernel encaminhar pacotes para ela. Ao contrário das chains do kernel, as chains de usuário não fazem parte do caminho que os pacotes percorrem no kernel.

# ...Chains...

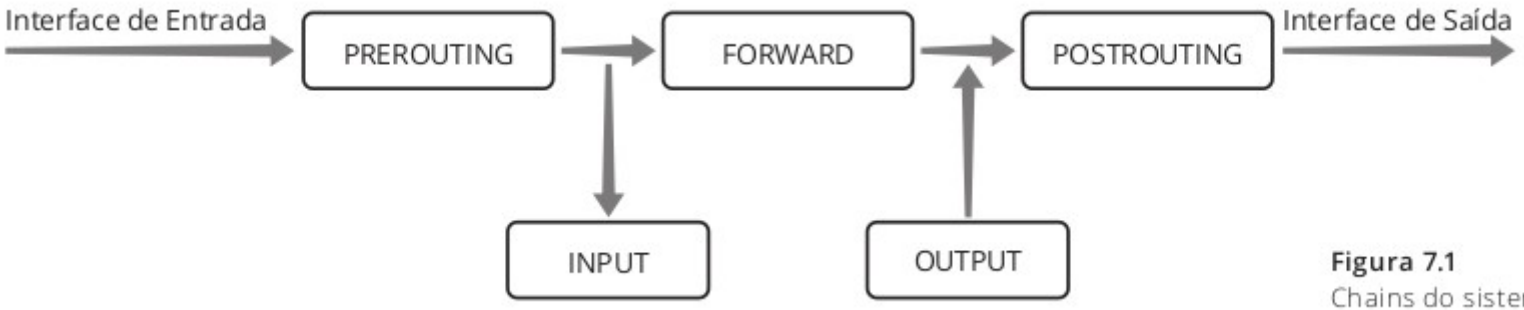


**Figura 7.1**
Chains do sistema.

Um pacote pode percorrer três caminhos dentro do netfilter:

- Pacotes que venham da rede com destino à máquina percorrem as chains PREROUTING e, em seguida, a chain INPUT.

- Pacotes que tenham origem na máquina percorrem a chain OUTPUT e, em seguida, a chain POSTROUTING.

- Pacotes que venham de uma rede com destino a outra rede (o firewall está atuando como um roteador) percorrem as chains PREROUTING, FORWARD e, em seguida, a POSTROUTING.

# ...Chains

Quando um pacote entra em uma chain, cada regra dessa chain é sequencialmente avaliada em duas situações:

- Até que o pacote combine com uma regra que contenha um alvo do tipo ACCEPT, DROP ou REJECT;
- Até que o pacote atinja o final da chain.

Nesse segundo caso, quando um pacote atinge o final de uma chain sem que tenha casado com alguma regra, é aplicada, então, a política padrão da chain.

# Tabelas

Tabelas são as estruturas onde as chains são armazenadas. O Linux possui apenas três tabelas, e as chains dessas tabelas contêm regras com funções específicas:

- Filter: tabela em que são colocadas as regras que filtram pacotes. Essa tabela possui as chains INPUT, OUTPUT e FORWARD.
- Mangle: utilizada por regras que alteram ou marcam pacotes. Possui as cinco chains: INPUT, OUTPUT, FORWARD, PREROUTING e POSTROUTING.
- Nat: utilizada para as regras de tradução de endereços de rede. Possui as chains PREROUTING, OUTPUT e POSTROUTING.

# IPTABLES

Iptables é o nome da ferramenta da interface do usuário que permite a criação de regras de firewall e NATs.

Apesar de, tecnicamente, o iptables ser apenas uma ferramenta que controla o módulo netfilter, o nome "iptables" é frequentemente utilizado como referência ao conjunto completo de funcionalidades do netfilter. **O iptables é parte de todas as distribuições modernas do Linux.**

Obs:Há uma versão do iptables, chamado de IP6Tables que é usado para configurar, manter e inspecionar as tabelas de regras de filtragem dos pacotes IPv6 no kernel do Linux.